Applying Packet Score Technique in SDN for DDoS Attack Detection

Sangeetha M.V.,
II ME CSE,
Department of Computer Science and Engineering,
Dr.MCET,
Coimbatore, India

Bhavithra J.,
Assistant Professor (SS),
Department of Computer Science and Engineering,
Dr.MCET,
Coimbatore, India

***Abstract*— Distributed Denial of Service (DDoS) remains to be one of the major issues against web servers and normal functioning of networks, because of freely available tools for generating attack and unprotected devices connected to the internet. Software Defined Networking (SDN) decouples controlling and packet forwarding mechanisms to reduce functioning overheads in a network and making whole network dynamically programmable, but it is vulnerable to DDoS and link congestion. DDoS defense mechanism includes DDoS detection, attack trace back and attack mitigation, of which detection is performed using various methods. In existing system, neural network is used to detect attack and it is trained with previously obtained attack dataset. By using neural networks, only specific attacks can be detected. In real time, detecting DDoS attack nearer to the attack source is essential. Collaborative mechanisms allow nodes within a network to share packet flow data, resulting in early detection of DDoS attack. In proposed system, Packet score method is employed to sense attacks that are spread by randomizing packet attributes by comparing flow characteristics during benign flow and the current traffic characteristics. DDoS attack is generated using Mininet in SDN environment to create nominal and current profiles. The proposed system is expected to improve accuracy of attack detection in early stages of attack when compared with neural networks based detection system.**

***Keywords*— SDN, DDoS attack detection, neural network, packet score.**

I. INTRODUCTION

One of the main threats to internet is DDoS attack or link congestion. DDoS attack is a kind of active attack in which a number of malicious systems or bots controlled by an attacker, flood inappropriate requests to a single server or system, keeping it busy and unable to serve legitimate requests. DDoS attacks can lead to loss of revenues, erode consumer trust, force businesses to spend fortunes in compensations and cause long-term reputation damage whereas launching a DDoS attack is very simple and inexpensive with tools available online. DDoS attacks are equally possible in SDN as that of traditional networks. SDN (Software Defined Networking) is the physical separation of the network control plane from the forwarding plane, where a control plane controls several devices. Usually, control plane has a controller which manages a number of switches in forwarding plane. Each switch has a flow table which contains flow entries associated with each flow through the switch and each flow entry is validated by corresponding controller. When attacker floods switches with multiple flows, controller may become unavailable at a point of time, leading to the network failure. DDoS defense mechanism involves attack detection, attack trace back and attack mitigation. Detecting DDoS attack can be done by comparison with previous attack patterns or by analyzing increase in packet count of each flow.

In section 2, related work is discussed and section 3 compares two kinds of detection methods. Section 4 briefs advantages and disadvantages of existing system. Section 5 details about proposed method where as in section 6, results and evaluation metrics are discussed.

II. RELATED WORK

A. DDoS Detection by Neural Network

Self-Organizing Maps (SOM) is an artificial neural network which transforms a given n-dimensional pattern of data into a 1- or 2-dimensional map or grid. It is unsupervised because the neuron network learns only with entry patterns, reorganizing itself after the first trained data and adjusting its weights as new data arrive [1]. In SDN, SOMs are distributed across the data plane along with OpenFlow switches to detect packet flooding at switch level itself. DSOMs are integrated with every switch individually and analyze flow entries at each switch. Yet this approach is not collaborative. [2]

B. DDoS detection by Collaborative approach

In this collaborative approach, three components namely, Monitor, Co-relator and Controller are used to perform attack detection, trace back and mitigation respectively. Monitors, distributed over a computer network, constantly observe the network traffic for any anomalies. Co-relators residing at Open Virtual Switches (OVS) respond to the alerts from monitors on demand. SDN Controllers themselves take actions to modify the network flows in attack mitigation. Monitor can employ different anomaly detection algorithms to flag a range of potential attacks.

Monitors have normal traffic behavioral profile and compare that with current traffic flow. [3]

PFS (Probabilistic Filter Scheduling), applied in traditional network, adopts Probabilistic Packet Marking (PPM), a general technique, which routers can use to reveal internal network information to end-hosts.PFS consists of four phases: 1) probabilistic packet marking, 2) filter invocation, 3) filter scheduling and propagation, and 4) filter revocation. In phase one, a filter router probabilistically marks its own IP address into the packet header. Then, in phase two, a victim collects and reconstructs the marking values to send a filter request. In phase three, the filter router receiving filter requests decides the best-k filters using a filter scheduling policy, and forwards the filters to upstream routers. Finally, when the attack stops, filters' score corresponding to the attacks decrease and the corresponding filters are eventually evicted from the filter router, which is phase four. [4]

Adaptive Probabilistic Filter Scheduling (APFS) follows the same procedure as that of PFS and uses a different packet marking technique [5] .In APFS, a filter router adaptively calculates its own marking probability based on three factors: hop count from a sender, the filter router's resource availability and the filter router's link degree. That is, a filter router that is closer to attackers, has more available resources, or has more connections to neighbours inserts its marking with a higher probability. These three factors lead a victim to receive more markings from more effective filter routers, and thus, filters are quickly distributed to effective filter routers. And, each filter router manages multiple filters using a filter scheduling policy that allows it to selectively keep the most effective filters depending on attack situations.

Possibility of attack traffic disguising as legitimate traffic is high in DDoS attack which may result in dropping legitimate packets wrongly. Statistical segregation method samples the flow in consecutive intervals and then the samples are compared against the attack state condition and sorted with the mean as the parameter, then the correlation analysis is performed to segregate attack flows from the legitimate flows. Attacks can be classified into low rate attack, constant rate attack, increased rate attack and intermittent rate attack. [6]

III. Comparison

When DDoS attack is detected by training neural network with previously obtained DDoS attack dataset, only specific attacks can be detected effectively. Specific attacks are identified by packets flows which have a particular attribute or group of attributes with values each counting huge number of packets than the normal flows. Generic attack is characterised by different kind of packet flows which cannot be covered under particular attribute and combining these flows contribute to huge number of packets that can result in DDoS attack.

IV. SD - ANTI - DDoS

A. Architecture

From the Fig. 1, coordination of SDN and anti DDoS mechanism can be observed. SDN has switches and controllers to manage network administration. A switch just performs packet forwarding or packet dropping based on the flow entries approved by the controller for the switch. One controller controls a number of switches based on the network capacity and layout, which can be configured by program. A controller that manages a switch decides which kind of packets must be forwarded or dropped by the switch and makes flow entries on the switch accordingly. When a switch encounters a new flow of packets that does not match flow entries in it, it intimates to controller about the new packet flow and waits for approval from controller in order to forward or drop the packets of new flow [7].

In order to reduce the bottleneck on the controller, a separate decision module is associated with it for knowing the credibility of new flow entries. With the help of this module, controller can easily inform switches about which packets to forward and which packets to drop. The reason for keeping a separate module for deciding on the legitimacy of packets is, when there is a flooding attack or a huge raise in flow of legitimate packets, each switch can have multiple new flow entries to be approved by the controller which can cause congestion between controller and switches, and controller have to decide on a number of flow entries in a very short duration which is not suitable for ensuring the security of the network.

It is clear that SD-Anti-DDoS takes care of DDoS detection, trace back and mitigation in consecutive steps. For attack detection, Back Propagation Neural Networks is used and for attack trace back, a lightweight trace back mechanism is employed that takes advantage of results from BPNN in previous step by analyzing flow statistics. In attack mitigation step, blocking attack flows by inserting new flow entries in the ingress port of the edge switch in the network that drop attack packets and cleaning malicious flow entries are done. Overall, existing system is a complete package of DDoS defence in SDN that concentrates on detecting attack as soon as possible. SD-Anti-DDoS or existing system utilizes OpenFlow communication protocol between controller and forwarding plane.

B. Collecting Flow Entries

In order to detect attack and trace back attack path, having flow information of packets from each switch is essential. Periodically, flow entries in each switch, managed by the controller, is snapped and stored into controller for further analysis. Flow entry log is used for identifying any malicious traces in incoming packet flows. Template of a flow entry is shown in Fig. 2, with which core aspects required for DDoS defence and features of packets can be distinguished. Header fields contain characteristics of incoming packet flow. Counters refer to the count

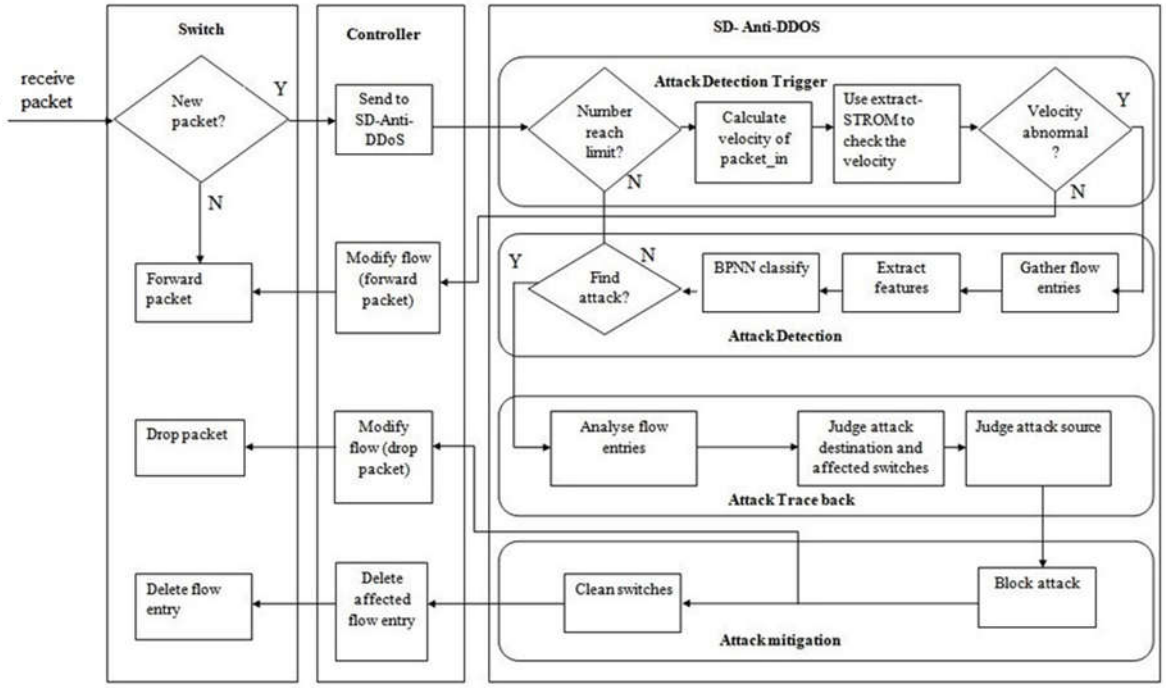

Fig. 1. Architecture of SD-Anti-DDoS

or number of packets that have arrived till the time of recorded flow entry. Actions represent whether to forward or to drop the packet flow in future.

C. *Extracting Features*

When there are specific DDoS attacks like SYN flood, UDP flood which contain very large number packets of a particular protocol with certain attributes set to same values, making the target to keep on listening or responding to these packets which leads to unavailability of service for legitimate users. In such scenarios, monitoring particular attribute values in flow entry is enough to make defense. Selecting appropriate attributes that constitute a particular attack type is important in detecting the attack correctly. Based on the service provided by the target system, types of DDoS attack that remain as big threats are identified and corresponding features are extracted from flow entries as a dataset to train the neural network in next step.

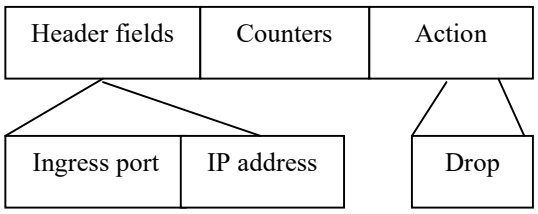

Fig. 2. Architecture of a generic flow entry

By observing values of specific packet attributes from table I, extracting features from flow entries can be understood. For example, in order to identify TCP SYN flood attack, protocol type and flag values are extracted from flow entries and analyzed. In table I, different type of DDoS attacks and attributes associated with them are listed.

TABLE I. ATTACK AND FEATURES

Attack Type	Attributes		
	Packet Protocol	***Flag / Port***	***Size (in bytes)***
TCP SYN Flood	TCP	Flag = 40	Rando mized
SQL Slammer Warm Attacker	UDP	Destination Port = 1434	131-140
DNS amplificati on attack	DNS	Des. Port = 53	60
Ping of Death	IP	Randomized but IP fragments are set to fake values	Exceed s 65,535
NTP attack	NTP	Des. Port = 123	90

V. DETECTION USING PACKET SCORE

Existing system has a downside of not addressing to the issue of identifying generic DDoS attacks. Moreover, identifying generic attacks by comparing attack signatures from previous attacks is difficult and not effective, as the current attack packets can hold attribute values randomized in a way that is very different from attack signatures in datasets and it will give poor results when applied in dynamically programmable SDN. This liability leads to the necessity of determining an attack based on recent behaviours and current traffic flow in the network, rather than using attack signatures collected from various sites. Attack signatures are useful only when the attack is specific. A collaborative approach is proposed to detect generic attacks in the dynamic SDN environment. Collaborative approach makes all nodes in a network to learn by co-operation and

decide about attack filters [8]. By this approach, proactive response to attack can be made, rather than reacting after an attack.

A. Profile creation

Each packet flow is recorded in the switch based on its attributes and number of packets having those attributes. This record is named as profile and it can be single nominal profile or pair nominal profile with respect to the number of attributes. In table II, TTL and Destination port are taken as attribute pairs to record packet flow during non-attack period.

TABLE II. PAIR NOMINAL PROFILE

TTL	*Destination Port*	*Number of packets or counter*
48	25	15
48	53	25
48	80	10
50	80	30
…	…	…

B. Packet Score Calculation

Based on the profile value, the pair which contributes to the attack is found and it is chosen to position filters to mitigate the attack. Comparing suspicious pair deviation and selecting it as score pair is done using following steps.

- Let S be the current switch and S', S'' and S''' represent switches at first, second and third hops from S. Let A, B, C, D, E, F represent six different attributes taken for profiling.
- Each of these switches has six single nominal profiles (SNP), six single current profiles (SCP), a pair nominal profile (PNP). Pair current profile (PCP) will be generated only after determining ScorePair of the switch.
- Packet count variation between SCP and SNP of the same switch (say S), yields suspicious pair of S as S(D,F) where D and F are most deviating in current profile when compared with nominal profile, among six attributes.
- If D and F were the randomly chosen attributes for pair nominal profiling in S, S(D,F) is said to be the ScorePair of S.
- If D and F were not chosen for pair profiling in S, then pair profiles of S', S'', S''' are taken in order and attribute matching is checked until ScorePair of S is found.
- If none of the pair profiles of S', S'', S''' have D and F as their pair profile attributes, own pair of S (attribute pair taken for pair profiling) is considered to be the ScorePair of S.

By following above steps, ScorePair of every switch is found. Based on this ScorePair attributes, Pair current profiles (ScorePCP) are generated at each switch. Each packet's score is calculated considering ScorePNP's corresponding value. If ScorePair is determined as A and B, then packet p with the attributes A = a_p and B = b_p will have the score S_p as follows

$$S_p = \frac{\text{ScorePCP}(A=a_p, B=b_p)/\text{TPCP}}{\text{ScorePNP}(A=a_p, B=b_{p,\dots})/\text{TPNP}} \quad (1)$$

Where

ScorePCP is the number of packets in current profile that have the property of a_p for attribute A and b_p for attribute B.

ScorePNP is the number of packets in the nominal profile that have the property of a_p for attribute A and b_p for attribute B.

TPCP is the total number of packets in current profile.

TPNP is the total number of packets in nominal profile.

The score of a packet needs to be compared with a threshold, Th. All scores are stored in a Score List and the threshold value, Th, is determined according to the cumulative distribution of scores. It is shown as symbolically CDF(Th) = ϕ where ϕ is the ratio of traffic that should be dropped. The fraction of traffic permitted to pass is 1-ϕ = Φ/ ψ where Φ acceptable traffic and ψ is the total current incoming traffic. Each packet's score value is compared with the threshold. If it exceeds the threshold, this packet is supposed to be malicious and discarded. Otherwise, it is forwarded to the destination.

VI. RESULTS AND DISCUSSION

In this section results are discussed. One of the main aims of this work is to discriminate attack packets based on the flow associated with the current system. By calculating packet score of each packet based on its attribute values, influence of each flow is measured and flows are discriminated based on threshold. Best threshold value can be selected by comparing the amount of attack packets discarded with the amount of benign packets forwarded.

Result of attack detection by neural network and packet score technique will be evaluated using the following evaluation metrics that use evaluation factors namely, True Negative (TN), True Positive (TP), False Negative (FN) and False Positive (FP). TP refers to packets classified as attack category that actually contribute to the attack. TN refers to packets classified as normal that are actually benign. FP refers to packets classified as malicious that are actually benign. FN refers to packets classified as benign that actually contribute to the attack.

Precision (PN) is the percentage of forwarded packets that are genuine.

$$PN = TP / (TP + FP) \quad (2)$$

Recal (RL) is the percentage of the legal packets were forwarded to the destination.

$$RL = TP / (TP + FN) \quad (3)$$

True Negative Rate (TNR) refers to the percentage of the attack packets that were dropped.

$$TNR = TN / (TN + FP) \quad (4)$$

Negative Predicted Value (NPV) displays the percentage of the dropped packets that were actually attack packets.

$$NPV = TN / (TN + FN) \quad (5)$$

Attack prevention efficiency (APE) measures how early the network can get rid of the attack packets. AP is the total number of attack packets, whereas dis_i shows the discard hop of the attack packet i and p_i shows the length of the path for the attack packet i from the source to the destination.

$$APE = 1 - \frac{\sum_{i=1}^{AP} \frac{dis_i}{p_i}}{AP} \quad (6)$$

TABLE III. CUMULATIVE SCORELIST

Score Pair(Source IP, Destination IP)	*Score (S_p)*
10.0.0.1 – 10.0.0.34	0.076952
10.0.0.6 – 10.0.0.55	0.097598
10.0.0.4 – 10.0.0.12	0.125047
⋮	⋮
10.0.0.23 – 10.0.0.21	0.500189
10.0.0.45 – 10.0.0.43	0.636604
10.0.0.56 – 10.0.0.61	0.750283
⋮	⋮
10.0.0.12 – 10.0.0.5	1.000378
10.0.0.11 – 10.0.0.78	1.167107
10.0.0.10 – 10.0.0.39	1.187948
⋮	⋮
10.0.0.52 – 10.0.0.9	2.080785
10.0.0.71 – 10.0.0.54	3.001133
10.0.0.30 – 10.0.0.7	4.251604

Table III shows a cumulative Score List generated from nominal and current profile of the score pair attributes (Source IP and Destination IP in this sample). Different values of threshold, Th, are determined from this list and corresponding packet discarding percentage is calculated. By this way, suitable threshold can be determined for every network periodically. Threshold determined for current profiling period can be used to fine tune the threshold of next profiling period.

VII. CONCLUSION AND FUTURE WORK

DDoS attack is detected using flow based collaborative method in SDN based on the nominal profile generated during non-attack period. In future, nominal profile can be monitored based on predefined constraints that are applicable to the specified networks like blocking packets of particular protocol and from particular networks or source. By that way, chance of DDoS attack on specific networks can be considerably reduced.

References

[1] R. Braga, E. Mota, and A. Passito, "A Lightweight DDoS flooding attack detection using NOX/Openflow", IEEE - Local Computer Networks , vol.1, pp.416-424, 2010.

[2] V. Trung Phan, K. Nguyen Bao, and P.Minho, "Distributed SOM: A Novel Performance Bottleneck Handler For Large-Sized Software Defined Networks Under Flooding Attacks", Elsevier: Journal of Network and Computer Applications, vol.91, pp. 14 – 25, 2017.

[3] C. Tommy, M.Xenia, L. Xiangyang, and X. Kaiqi , "An SDN-supported collaborative approach for DDoS flooding detection and containment", IEEE - Military Communications Conference, vol.1, pp. 659-665, 2011.

[4] S. Donwon, and P.Adrian, "PFS: probabilistic filter scheduling against distributed denial-of-service attacks", IEEE - Local Computer Networks, vol.1, pp. 9-17, 2011.

[5] S. Donwon, and P.Adrian., "APFS: adaptive probabilistic filter scheduling against distributed denial-of-service attacks", Elsevier: Computers & Security, vol.39, November, pp. 366-385, 2013.

[6] J. Udhayan, and T.Hamsapriya, "Statistical segregation method to minimize the false detections during DDoS attacks", International Journal of Network Security, vol.13, Issue:3, pp.152–160,2011.

[7] Yunhe C. et al, "SD-Anti-DDoS: fast and efficient DDoS defense in software-defined networks", Elsevier - Journal of Network and Computer Applications, vol.68, pp. 65 –79, June 2016.

[8] Kübra K. and Fatih A, "A distributed filtering mechanism against DDoS attacks: ScoreForCore", Elsevier – Computer Networks, vol.108, pp. 199 –209, October 2016.

[9] Kübra K., Gurkan G., and Fatih A., "Defense mechanisms against DDoS attacks in SDN environment", IEEE Communications Magazine, vol.55, Issue: 9, pp. 175 –179, 2017.